

Original Article

Classes of socio-technical hazards: Microscopic and macroscopic scales of risk analysis

Stuart Anderson and Massimo Felici*

School of Informatics, The University of Edinburgh, Edinburgh, EH9 3JZ, UK.
E-mail: mfelici@inf.ed.ac.uk

*Corresponding author.

Abstract Understanding risk in technology involves analyzing of diverse socio-technical aspects and their interaction. This is due to the risk complexity, which often inhibits the effectiveness as well as the applicability of purely technological risk analysis (as distinct from organizational risk analysis). Diverse accounts of risk in technology advocate and argue about different aspects of technology risk. Although a first insight of these accounts might result in controversial understandings of risk, a further analysis highlights how they often point out similar (or compatible) conclusions about technology risk. This paper draws on diverse accounts of technology risk. Multidisciplinary perspectives of risk allow us to identify and define three classes of socio-technical hazards: *boundary*, *evolutionary* and *performativity* hazards. These classes enhance our understanding of technology risk. They highlight out how diverse accounts of risk refer to different granularities of risk – (technological) microscopic and (organizational) macroscopic levels of risk analysis. The benefit of understanding and capturing socio-technical accounts of risk is twofold. On the one hand, it points toward an interdisciplinary account of technology risk. On the other hand, it provides a means for structuring risk analysis according to multidisciplinary perspectives. The combination of different levels of risk analysis enhances our understanding of the risk of technology innovation with respect to classes of socio-technical hazards.

Risk Management (2009) 11, 208–240. doi:10.1057/rm.2009.7

Keywords: technology risk; multidisciplinary and interdisciplinary risk; microscopic and macroscopic risk analysis; socio-technical hazards; boundary; evolutionary and performativity hazards

Introduction

The study of *technology risk*, or risk in technology, involves the analysis of how technology exposes society to different threats or hazards. The *risk society* is concerned with how technological hazards affect different groups (Douglas and Wildavsky, 1982; Beck, 1992). Risk complexity manifests in how technology hazards propagate across organizational or social boundaries (for example, division of labor, social classes and so on (Douglas and Wildavsky, 1982; Perrow, 1999). Knowledge about technology informs debates, empowers social groups and allows them to position with respect to technology risk (Beck, 1992). Various studies (for example, Douglas and Wildavsky, 1982; Beck, 1992; Neumann, 1995; Perrow, 1999) investigate and define a broad spectrum of socio-technical accounts of technology risk. These range from a *microscopic* (for example, how individuals behave with respect to technology and perceive risk) to a *macroscopic* (for example, organizational, social, socio-political, environmental and so on) analysis of technology risk.

Classifications of risk studies (for example, see Le Coze, 2005, 2008) highlight how different accounts of risk lead to different understandings of socio-technical problems. The combination of different levels of investigations – for example, ‘micro/meso/macro’¹ – together with diverse types of models and approaches – for example, ‘normative (or prescriptive)’ as opposed to *descriptive*² – allows a characterization of different risk problems (Le Coze, 2008). On the one hand, the interpretation of ‘complex causalities’³ that characterize ‘complex interactions’ (Perrow, 1999; Felici, 2006a) triggering ‘unpredictable’ failures (or failure modes). On the other hand, the epistemology of the investigations of failures draws backward the causalities leading to accidents (Le Coze, 2008). These dimensions, that is, micro/meso/macro and normative/descriptive, identify a framework for the classification of the modeling approaches underlying the investigations of past accidents (Le Coze, 2008). Similarly, it is possible to identify different organizational levels, from ‘closed system models’ to ‘open system models’ (Le Coze, 2005), for the classification of safety approaches and the underlying models with respect to different social levels of analysis.

These classifications position research and investigation methodologies according to ‘topologies of socialities’ (for example, micro/meso/macro) and ‘system boundaries’ (for example, closed as opposed to open system models; Le Coze, 2005, 2008). Disciplinary boundaries between accounts inhibit and narrow the scope of analysis of technology risk. This often limits our understanding of technology risk and its underlying mechanisms as a whole. At its simplest, there is a disconnect between different levels of granularities. Drawing similarities and links between diverse accounts of risk supports cross-fertilization between scientific and practitioner communities, who seek to understand risk in technology innovation. Unveiling contingencies between

the social and the technical enhances our understanding of where socio-technical risks reside. An interdisciplinary account of *emerging technology risk* seeks to establish links between technical and social accounts of technology risk. But, social accounts of risk can be very different, for example, the economic account begins with the 'individual', whereas the sociological begins with the 'group' – for example, contrast a 'market' view of risk with a 'cultural' view of risk. This paper discusses these links in terms of 'complex' *socio-technical hazards*. In order to establish such links, the focus is on the following questions (which are important, but not exhaustive):

- (i) How does technology cross organizational (for example, social and cultural) boundaries? How does technology expose organizations to risk across their boundaries? Understanding the underlying mechanisms about how technology supports diverse forms of social organizations allows us to address the risk associated with 'unbounded' technology (or open system models).
- (ii) How does technology innovation capture evolutionary processes? Social interaction shapes technology. In order to understand the contingencies between technology innovation and evolutionary processes (characterized by social interaction), it is necessary to unveil how technology innovation affects work practice.
- (iii) How do communities gather together around technology? It is necessary to understand how communities of practice affect technology development. Accidentally, technology innovation exposes communities of practices to reduce diversity and increased common vulnerability. Hence, it exposes communities of practice to 'complex' system failures (or complex causalities). Understanding the contingencies between the social and the technical requires us to investigate mechanisms of failure propagation across organizational boundaries.

This paper draws on accounts of risk that contribute toward an interdisciplinary understanding of emerging technological risk. In particular, it points out work that falls into the different scales, that is, microscopic and macroscopic. The potential benefit is an interdisciplinary study that links these two scales of analysis. A review of relevant work outlines and emphasizes how multidisciplinary work problematizes the relationship between scales of analysis. It also assesses the promise of new tools and techniques that arise from interdisciplinary work on emergent risk in socio-technical systems. This paper articulates emerging technological risk in terms of three classes of socio-technical hazards, namely, *boundary hazards*, *evolutionary hazards* and *performativity hazards*. It explores these classes of socio-technical risk, which arise from the interdisciplinary study of technological risk. These classes of socio-technical hazards support risk analysis from microscopic to macroscopic scale and vice versa.

Hence, they provide an account of technology risk as a whole. They look at how diverse risk perspectives affect each other. This paper is organized as follows. The next section reviews accounts of technology risk. This paper then identifies and describes the three classes of socio-technical hazards. It, finally, discusses how these classes relate to microscopic and macroscopic scales of risk analysis.

Risk Dimensions

Reviewing accounts enhances our understanding of technological risk. It supports the development of a multidisciplinary (or interdisciplinary)⁴ account of technological risk. It is important to analyze diverse aspects contributing toward *multidisciplinary risk accounts* (Aven and Kristensen, 2005). On the one hand, it extends and complements engineering accounts of technology risk. On the other hand, it overcomes the limitations of individual disciplines. It encourages and stresses bridges between, for instance, social and engineering accounts of technology risk. Moreover, it makes social dimensions of risk accessible to practitioners, and vice versa. Linking diverse accounts and relevant work in risks of technology innovation is more explanatory rather than solutionary. It provides ways of questioning technology innovation with respect to accounts of risk. It is possible to identify a wide spectrum of technological risk, from technical to social analysis of risk.

Analyzing the relationships between accounts of technology risks allows us to understand subtle technological complexities. Understanding the nature of *technological risk*, or *risk in technology*, requires us to uncover these complexities in order to develop a more refined account of technology risk. It highlights how accounts of technological risk relate to each other. Understanding them and how they relate to each other enhances our ability to structure and perform risk analysis to different levels of granularity. The underlying assumption is that different accounts of technology risk relate to different levels of analysis.

This section highlights different aspects of technology risk. It identifies an understanding of technology risk that contributes toward an interdisciplinary account of *emergent technological risk*. The review covers from technology to social accounts of risk in order to emphasize different levels of analysis in the underlying approaches and results. The outcome is a set of relationships among studies of risk that see a holistic account of technology risk emerge. Finally, it advocates future research and practice toward interdisciplinary accounts of technology risk.

Technology risk

Technology carries related risks, which originate from many engineering aspects (for example, system development, operation and use and so on). From an engineering viewpoint, it is useful to distinguish between a *hazard* and its associated *risk*.⁵ The definitions of hazard, risk, system and environment are

the bases of causal analysis of accident investigations (Johnson, 2003). The main engineering risks fall into two categories of sources of problems: *system development* (for example, requirements definition, hardware and software implementations, evolution and so on) and *system operation and use* (for example, natural environmental factors, infrastructural factors, software misbehavior, human limitations in system use and so on; Neumann, 1995). Note that the classification has a principal technical viewpoint.

Engineering methodologies, in particular in the safety-critical domain (Leveson, 1995; Storey, 1996), address some engineering risks, although they provide limited clarification in understanding and identifying subtle emerging socio-technical risks. The increasing dependence on technology justifies an increasing interest in system properties. For instance, the study of features, such as reliability and safety, has contributed to the advance of engineering methodologies addressing technological issues (Neumann, 1995). The analysis of failures in safety-critical domains allows us to understand different pitfalls in engineering computer systems (Leveson, 1995). For instance, it stresses the differences and contingencies between safety and reliability properties of systems. Research in *dependability*⁶ has developed various methodologies 'to specify, design, implement and exploit systems where faults are natural, expected and tolerable' (Arlat, 1998). Unfortunately, technical arguments for system dependability often face subtle socio-technical complexities and contingencies (Felici, 2006a).

The analysis of *accidents* highlights features characterizing technology risk. System features of *complexity* and *coupling* form a framework for the analysis of system risks (Perrow, 1999). The framework classifies systems according to complexity of interaction (that is, *linear interactions or complex interactions*)⁷ and *coupling* (that is, loosely or tightly) between components (Perrow, 1999). It highlights three main categories of high-risk systems depending on the severity and complexity of risks, as well as, the possibility of effectively addressing those risks (Perrow, 1999). An interesting point is to which extent the framework embraces socio-technical systems as a whole – *Are complexity and coupling also related to organizational structures* (for example, *management structures* and so on) *for socio-technical systems?*

The classification of systems according to the complexity/coupling framework is in agreement with technically informed risk analysis, although *social and cultural rationalities* undermine the risk classification influencing *risk perception* (Douglas and Wildavsky, 1982; Perrow, 1999; Slovic, 2000) and *risk amplification* (Health & Safety Executive, 2001a,b, 2002). This aspect characterizes the social and cultural rationalities, which judge dreads and uncertainties with respect to many factors (for example, implications for future generations). Despite this, the coupling/complexity classification takes into account victims of system risks, uncertainty and other factors that point to drivers for public judgment. They influence the reasoning of any informed and

knowledgeable person as well as the general public. The complexity/coupling framework takes into account three main clusters of interrelated judgments: (Perrow, 1999) *dread risk* (for example, lack of control over the activity, high catastrophic potential and so on), *unknown risk* (for example, unknown, new, delayed and so on) and *societal and personal exposures*. Although social aspects undermine the classification and identification of risk, it is still possible to identify general policies (for example, of centralization or decentralization) defining authority and responsibility in order to mitigate some risks due to tightly coupled components exhibiting complex interactions (Perrow, 1999). This stresses how social structures and mechanisms affect risk (for example, risk perception, risk exposure and so on) as well as the engineering of technology innovation.

Risk in engineering knowledge

Various engineering domains have investigated and validated the thesis of *Engineering as Knowledge* (Vincenti, 1990). A historical account of engineering highlights activities that contribute to the acquisition of knowledge into technical systems. On the one hand, technical systems are repositories of engineering knowledge. This view allows us to distinguish between engineering and applied science, hence, engineering as involving activities of designing innovation. On the other hand, from a knowledge perspective, engineering is reduced to the design of technical systems. It is possible to distinguish two different situations: *normal* and *radical designs*. *Normal design* is the design of normal technology based on what technological communities do. *Radical design*, as opposed to normal design, involves the design of technology under *knowledge uncertainties*.

Knowledge uncertainty

Engineering technology is, therefore, a learning process (Vincenti, 1990). The *engineering learning process* involves (seven) different interactive elements (for example, familiarization with problem, development of instruments and techniques, measurement of characteristics, assessment of results and so on) forming a complex epistemological structure. Despite the elusive order of the learning process (in terms of the interactive elements), engineering technology involves an accidentally iterative *variation–selection model* for the growth of engineering knowledge. Different activities contribute toward generating engineering knowledge. The variation–selection model involves three main cognitive activities, that is, *searching of past similar experiences, incorporating innovation features and selecting design alternatives* most likely to work, which characterize engineering knowledge and its growth. First, searching for past experiences in which engineering knowledge was successfully used. On the other hand, failures represent a source of engineering knowledge too (Petroski

1982, 1994). Second, the conceptual incorporation of engineering knowledge into local artifacts. This highlights two features of engineering knowledge. Engineering knowledge is the result of communities of practice adopting (or naturalizing) artifacts. It emphasizes knowledge as *distributed cognition* (Norman, 1993). Engineering knowledge falls into various categories: *fundamental design concepts, criteria and specifications, theoretical tools, quantitative data, practical considerations and design instrumentalities* (Vincenti, 1990). These categories form engineering knowledge consisting of *descriptive knowledge, prescriptive knowledge and tacit knowledge contributing toward explicit knowledge or procedural knowledge*.⁸

Knowledge growth in engineering characterizes epistemic accounts of technological innovation (Vincenti, 1990). Emerging technological risk relates to *uncertainty in engineering design knowledge* with respect to technical as well as environmental factors (for example, social organizations, communities of practice, evolving operational profiles, increasing performance requirements and so on), although knowledge uncertainty provides a partial account of technological risk (Douglas and Wildavsky, 1982). It is necessary to select those design solutions that are likely to function in future (foreseen) operational conditions. It is evident how uncertainty in engineering design knowledge involves an extent of risk. Evolutionary design processes intend, to some extent, to address knowledge growth, uncertainty and three main underlying *evolutionary drivers* (or *drivers of technology evolution*): *functional failure, presumptive anomaly* and the need to *reduce uncertainty* in design knowledge (Vincenti, 1990). All of these drive different methodologies, which deal with different kinds of mistakes or errors (for example, not understanding the environment, faulty process, faulty execution of process and so on). Functional failures are characteristics of increasing performance requirements under unforeseen operational conditions. *Failures*, or *errors*, represent a source of engineering knowledge (Petroski 1982, 1994), although design faults represent a threat for system dependability (Avi-zienis *et al*, 2004). The evolutionary process of searching from knowledge and designing innovations is supported by the analysis of past design errors. *Errors*, or *faults* (Arlat, 1998; Avi-zienis *et al*, 2004), in design represent a source of engineering knowledge (Petroski 1982, 1994). *Learning by mistakes* is a fundamental paradigm of engineering. Therefore, growth in engineering design knowledge is a compound learning process (for example, *social learning involves learning by interacting or learning by doing* with respect to technology (Williams *et al*, 2005)).

Knowledge negotiation

Technology, or engineering knowledge, registers social (for example, organizational) interactions into structured designs. *The system approach*, for example, highlights how heterogeneous artifacts form and let technology to emerge resulting into systems (Hughes and Hughes, 2000). Engineering knowledge

emphasizes how technological artifacts emerge as result of design activities giving rise to *technology trajectories*, or what it seems the 'normal' *evolution of technology*, consisting of 'subsequent' *technical changes* (MacKenzie 1990, 1996). On the other hand, sociological accounts of engineering knowledge highlight the *social shaping of technology*.⁹ Social processes of technological change emphasize a notion of *heterogeneous engineering* as (design) solutions in search of problems, rather than problems to be solved or problems in search of solutions (MacKenzie 1990, 1996). Separating knowledge from technology is just an artificial segmentation for representing cycles of discoveries and innovations. Innovation cycles involve technological evolution with respect to *engineering knowledge, technology and communities of practice*. Communities of practice shape technology innovation by selecting and adopting available technology and knowledge. Eliminating the relation of communities of practice with respect to technology and (engineering) knowledge restrict the understanding of discovery and innovation to classical engineering deterministic views giving rise to the controversial *paradox of proving the correctness of technology* (MacKenzie, 2001a). Social interactions, shaping technology, allow us to investigate how technology pervades work practices, hence, understanding communities of practice with respect to technology. On the one hand, social shaping of technology highlights risk perception of technological evolution. On the other hand, technological evolution is a potential hazard that disrupts work practice. However, it is possible to analyze and capture technology trajectories in order to understand design decisions with respect to technological evolution.

Knowledge granularity

Organizations often advocate technology innovation as a means of improving performance (for example, increased safety). Unfortunately, uncontrolled and misunderstood introduction of new technology could have controversial results in particular domains (Perrow, 1999). Presumptive anomalies highlight uncertainties over future operational conditions or requirements, which may expose the limitations of current systems. Design processes, finally, seek to reduce uncertainty by specific activities (for example, system testing). On the other hand, the characterization of engineering knowledge emphasizes that creating knowledge and reducing uncertainty are community activities depending on work practices and (social) interactions. Unfortunately, 'information difficulties',¹⁰ from an organizational viewpoint, represent 'barriers to organizational learning' (Pidgeon and O'Leary, 2000). These issues often concern a lack of *safety culture* (for example, see Health & Safety Laboratory, 2002; Health & Safety Executive, 2005 for a review of relevant work on safety culture) within organizations. On the other hand, addressing issues of organizational learning requires the integration of diverse approaches and perspectives toward socio-technical accounts of technology risk (see Atkinson, 2001 as an

example of socio-technical approach tailored for a specific domain or organization).

Central to the growing of engineering knowledge is the role of communities of practices that highlight the epistemological nature of engineering knowledge. Their activities and interactions are major drivers for the creation of engineering knowledge as technology innovation. Empirical analyses of work practices (Ackerman and Halverson, 2000, 2004) highlight how organizational knowledge relates to technology innovation (D'Adderio, 2003a,b; D'Adderio, 2001). Research¹¹ often debates of what constitutes local – *micro* – and global – *macro* – knowledge. Although it is often difficult to draw clearly a distinction between the local and the global levels, it emphasizes the analysis of organizational knowledge at different levels of granularity, for example, at the micro level, where individuals use technology artifacts enabling organizational memory to be reused, or at the macro level, where groups of people (or communities of practice) shape technology artifacts enabling organizational knowledge to be shared. Global contexts are those in which knowledge cannot be recontextualized quickly (or at all), because there are no mechanisms to achieve this. Local contexts are those in which knowledge can be recontextualized when necessary (often by informal means).

Organizational (memory) knowledge, however, involves both the (technology) artifacts storing knowledge and the processes enabling knowledge management and reuse (Ackerman and Halverson, 2000, 2004). Taking into account a social perspective of technology, therefore, allows us to investigate about how organizations '*transfer*' knowledge into technology innovation (D'Adderio, 2003a). This is in accordance with the social shaping of technology theory, which emphasizes how technology innovation is the results of heterogeneous engineering shaping socio-technical systems. Failing to understand the underlying mechanisms and their social perspectives poses organizations to socio-technical hazards, may be, emerging as undependabilities, such as, technology failures, mispractices ('human error') or reduced services.

Human dimensions of technology risk

Technology accounts of risk have limitations in uncovering complex failure mechanisms. For instance, a narrow viewpoint of analysis focusing on technical systems could be misleading and erroneous in classifying 'system failures' due to 'human error' (Hollnagel, 1993; Johnson, 2003). At the microscopic level, 'human errors' capture interaction issues. On the one hand, technology interaction (for example, human-machine interaction) highlights subtle contingencies between human performance and (system) reliability. Understanding system failure modes allow users, or human operators, to develop *trust* in technology and *confidence* in (their) work practices and understanding

of the system. Social accounts of trust (for example, see Felici, 2006b, 2007; Bottitta and Felici, 2006 for an account of trust) and risk perception (Douglas and Wildavsky, 1982; Slovic, 2000) stress the interaction between trust, risk and knowledge. Therefore, a social viewpoint provides a convenient intersection between risk, trust and technology. The different relationships (for example, independence, mediation and moderation) between trust and risk affect emergent behaviors. These relationships between risk and trust highlight different behaviors of socio-technical systems. The interaction between trust and risk perception provides the basis for an analysis of social aspects of technology. The characterization of trust and risk suggests that the underlying constructs interact in the formation of trust and the perception of risk. This interaction originates in social aspects of trust and risk. For instance, this gives rise to the phenomenon of *risk homeostasis* – the result of over trusting technology – consisting in a reduction of risk perception due to advances in technology (Hollnagel, 1993). The level of risk perception is constant, although increasing demands on performance push the system to work close to hazardous conditions. On the other hand, the growing complexity of technology and the tight coupling of technology affect risk perception and expose human performance to system failures (Perrow, 1999). The problem is then twofold. The first concern is with the management complexity of systems. The second one is the management coupling of these complex systems. For instance, this is the case in software development for some classes of system. However, many of the more successful large-scale systems consist of potentially quite complex components that are socially managed in a lightweight manner and have relatively low coupling. Many embedded systems do meet the complexity/coupling criteria, because they have a high management complexity and have tight coupling – for example, modern automotive systems – but as these become socialized and black-boxed, the management complexity diminishes.

An effective *human reliability analysis* (HRA) requires an understanding of *human cognition* (Hollnagel, 1993), that is, it is necessary to understand and analyze those cognitive processes characterizing human behavior. The *distributed cognition* theory highlights how distributed artifacts enable human cognition as a negotiated process within communities of practice (Norman, 1993; Bowker and Star, 1999; Halverson, 2002). *Bounded rationality* is another aspect of human cognition (Gigerenzer *et al*, 1999). It provides an alternative perspective to probabilistic approaches of knowledge. Reasoning and decision-making processes often rely on limited information and constrained environmental conditions. Understanding bounded rationality allows us the identification of fast and frugal heuristics, which provide a characterization of human reasoning and decision-making in real situations exhibiting limited computational capacities and resources. The analysis in situated cases identifies in fast and frugal heuristics valuable tools for understanding the processes of reasoning and decision-making under constrained knowledge.

The performance of fast and frugal heuristics exhibits some sensibility to information structure (or information ecology), that is, how information is distributed or organized in the environment. Therefore, at the microscopic level, cognition involves processes and artifacts characterizing technology interaction. At the macroscopic level, cognition involves negotiation (within emerging social networks; Nardi *et al*, 2002). To which extent negotiation takes place, it depends on group socialities (Douglas and Wildavsky, 1982). Different types of individuals or groups (for example, ‘individuals’, ‘egalitarians’, ‘hierarchists’ and ‘fatalists’ (Douglas and Wildavsky, 1982; Health & Safety Executive, 2002) have certain kinds of disposition to act in a particular way (in say how they recognize and mitigate dangers) that arise from their Grid/Group positions and rules. This, again, stresses the social shaping of technology. Moreover, a lack of understanding of the different hierarchical layers, granularity of interaction, exposes organizations to emerging technology risk (Reason, 1997).

Risk society

The traditional view is that technological systems have flaws, hence, on the basis of the frequency of manifestation and severity of the consequences, risk assessment drives the management of flaws. Risk in technology, unfortunately, is more heterogeneous, difficult and complex to capture, because technology is deeply embedded in social and organizational contexts. This complicates the analysis of risk associated with socio-technical systems. The *risk society theory* provides a social account of risk (Beck, 1992). Although the risk society provides a partial account of socialities, or social mechanisms, of risk (Löfstedt and Frewer, 1998; Mythen, 2004), it analyzes the shift in modern society from the social production of wealth to the social production of risk (Adam *et al*, 2000). Analyzing the distribution problems and conflicts arising emphasizes the nature of techno-scientific produced risks. The risk society is, therefore, concerned with trade-offs involved in the systematic production of risks and hazards as part of *modernization* (Latour, 2003) – often involving technology innovation. The aim (of risk assessment, management and mitigation) is to minimize, prevent and mitigate arising risks or ‘latent side effects’ of modernization. For instance, the risk society is characterized by the production and trade of hazards. The *information society* (IS) is, therefore, a particular instance of the risk society. An emergent market in the ‘modern’¹² IS is the one that exploits security vulnerabilities (Anderson and Moore, 2006). Risk society captures and explains the economics of vulnerabilities.

An important characteristic of modernization is its ‘reflexivity’ (Latour, 2003; Beck *et al*, 2003). The reflexivity of modernization, unfortunately, may have negative effects and support negative forces damaging the risk society itself. The modern economic society exhibits the features of the risk society

(MacKenzie, 2006). The 'performativity'¹³ of the modern economic society presents similarities with the reflexivity of the risk society. Hence, economic and technology societies are expressions of the risk society. They act more as a risk distributing society rather than a wealth distributing society. The scale of risk acquires a global dimension. The question is then: *where is the risk in technology innovation?* For instance, modern society depends on technology. However, it is possible to distinguish different types of risks (for example, 'perceived through science', 'perceived directly' and 'virtual risk' Health & Safety Executive HSE, 2002), which require different types of risk management. In particular, technology risk analysis provides input to the class of risk perceived through science. The way people perceive and behave with respect to arising technology risk makes technology society more of a risk society. However, often debating about risk without a clear 'definitive' position gives rise to virtual risk. The concept of risk is directly influenced by the concept of *reflexive modernization*. Accidents relate to the people affected. That is, it is important to understand how people position with respect to (technology) risk in the risk society.

The position with respect to risk crosses organizational boundaries, classes and divisions of labor. A cultural theory analysis of risk perception would say the High Grid Low Group cultures would take a fatalistic view of all dangers, whereas Low Group Low Grid cultures would see individual hazards as more important than risks to society (for example, argue that global warning is not a risk but an opportunity for the right person; Douglas and Wildavsky, 1982). The fact is that High Grid Low Group cultures are often low income, low status, low class (that is why they need to be controlled). The risk society differs from the class society. There are several inequalities that stress the distinction between class and risk society. The risk society, for instance, spreads across class, social and cultural boundaries. Knowledge distribution creates awareness of risk. Knowledge is embedded in distributed resources, which are accessible regardless from class and culture. The more accessible resources are, the more likely people acquire knowledge about risk. Similar considerations account in the analysis of technology complexities (Perrow, 1999) – *how does technology complexity relates to its risk? What are the social implications (with respect to risk) of technology?* On the one hand, considering, for instance, technology, environment and management, it is quite possible to have very highly complex technologies that are fairly easy to manage (for example, the phone network is complex yet involves relatively low management complexity – but this might be changing because companies are looking to make management more complex to squeeze increasing performance out of the network). On the other hand, despite technology, barriers provide mechanisms to identify 'acceptable values' of risk (on which concepts, such as ALARP (as low as reasonably practicable), are developed: Storey, 1996), risk society exposes the limitations of

organizational (for example, 'Swiss cheese') models of defenses (Beck, 1992; Reason, 1997).

Knowledge (hence, technology) acquires a different role enabling political and social debates in the risk society. Knowledge about risk consists of projections of dangers (or hazards) to the future. For instance, the Y2K (year 2000) hazard concentrated the attention of people on potential risks of technology systems (Perrow, 1999). Unfortunately, risk involves uncertainty in knowledge. Therefore, uncertainty exposes the limitations of the *calculability of risk* (MacKenzie, 2001a). That is, the calculability of risk is a socio-technical problem, rather than a purely technical one. Uncertainty characterizes the risk society. Moreover, the risk society exhibits particular features. First, modernization involves new types of risks. Second, social structures (or positions) expose people to risk differently. Risk exposure crosses the classical organizational boundaries or divisions of labor. Because of the reflexive nature of the risk society, identifying trade-offs and negotiating knowledge involve strategies and policies giving rise to social as well as political debates (or decision-making games). Knowledge about risk, therefore, acquires a critical social and political power, because it enables and positions (that is, empowers) people with respect to risk. Finally, hazards and risks (or consequential catastrophes) have the potential to influence risk perception. Moreover, risk perception is subject to the phenomenon of social amplification of risk (Slovic, 2000). Therefore, it is mandatory to include both social and cultural aspects in the formulation of technology risk. That is, it is unrealistic to characterize technology risk without including emerging social structures and mechanisms.

The cultural theory of risk shows how different constitutions of social groupings within an organization behave with respect to hazards (Douglas and Wildavsky, 1982). The concepts of safety culture or safety climate identify and describe 'shared corporate values within an organization which influences the attitudes and behaviours of its members' (Health & Safety Laboratory, 2002). Safety culture highlights about how different organizational or social structures,¹⁴ that is, groups select, hence, perceive risk (Douglas and Wildavsky, 1982). This characterization of risk perception, with respect to social structures, highlights a correlation between social structures and risk (perception), hence, the presence of subcultures.¹⁵ For Instance, highly structured and regulated groups perceived risk differently than unorganized groups, who feel a lack of control over risk selection. The *psychometric paradigm* of risk perception highlights similar results (Slovic, 2000). In contrast to Cultural Theory, it advocates a quantitative and qualitative framework for studying risk perception. An increase in risk perception is twofold. On the one hand, risk may have increased. On the other hand, our knowledge of risk may have increased. Risks therefore relate to knowledge.

Much of this broader socio-technical analysis of risk casts light on risk in organizations. The analysis of potential risks in organizations requires us to

understand and focus on how the dominance of particular groups de-emphasizes certain classes of risk. For example, in security standards, one might expect to see High Grid High Group culture dominating standards formation. This might suggest standards would arise that emphasize the role of deviants as a source of risks. This is very evident in security risk assessment guidelines (for example, Stoneburner *et al*, 2002), which emphasize deviants and tends to neglect internal threats due to excessive diligence of some groups (for example, system administrators in applying the latest patches that might deny a legitimate user access to some service). Similar aspects emerge in the study of the economics of information security in which emerging network topology and behavior (for example, 'strategy proof') affect security aspects (Anderson and Moore, 2006).

Further understanding these types of mechanisms in the design of technology innovation allow the identification of organizational risks that might otherwise be overlooked. Organizations comprise many different groups, whose risk perception may differ radically and whose needs for, and attitude to, system change also varies depending on role and environment. As different participants in an organization potentially have very different perception of the existence and severity of risks, it is necessary to consider issues of risk perception to help manage risk in complex organizations. It is important to highlight how socialities explain, understand and perceive risk, in particular, with respect to technology innovation. This requires us to develop mechanisms for handling risk arising for ongoing processes of change in organizational systems, that is, how to manage the risks of change in complex technology (Borodzicz, 2005).

Classes of Socio-Technical Hazards

The review of the diverse risk dimensions draws over various multidisciplinary accounts and highlights the complex nature of technology risk. This section further articulates the analysis of technology risk. It describes three classes of socio-technical hazards, namely, *boundary hazards*, *evolutionary hazards* and *performativity hazards*, which relate to our three main points of analysis.

First, it is important to take into account that organizations have many cultures and to understand how technology, hence, risk too, crosses organizational boundaries. Organizational cultures need to meet to achieve specific objectives. At the meeting points, knowledge or information structures are constructed; these can be abstract or concrete but they provide the interface necessary to get a range of tasks done. They are points of conflict and tend to be quite highly specialized to the job in hand. They are also a much less rich repository of situational knowledge than is typical within a single group (that is, the shared interpretation across groups is weaker than

interpretations inside a group). The intersection of different communities of practice often identifies *boundary objects* as knowledge repositories (Bowker and Star, 1999). Boundary objects are affected by those changes happening to those tasks that they are intended to support. Classifications are a good example they chop up experience into classes, but if things change and we need to chop up experience differently then we struggle to get any continuity. Classifications, like information systems or infrastructures, are ubiquitous and pervasive in many professional and application domains. They are the result of technical as well as social and political struggles addressed over the years. Moreover, change in one group that shares a boundary object can affect the way it is used by everybody. Standardization or innovation strategies expose organizations to a set of hazards involving boundary objects, or infrastructures, hence, Boundary Hazards. Analyzing and understanding how organizations use diverse technology artifacts reduces their exposure to these hazards.

Second, it is important to analyze how technology innovation both shapes and is shaped by evolutionary processes involving social interaction. It is also important to understand the level of risk an organization experiences during technological innovation. Another class of technological hazards, therefore, is the one that involves *evolutionary hazards* (for example, evolving work practices, understanding technology trajectories and judging moving targets). Technology innovation is driven to some extent by technological advancements. Technology trajectories emerge as results of evolutionary negotiations involving communities of practice. Capturing these shifts enhances our ability of constructing, reusing and changing technology arguments (for example, safety arguments). Understanding mechanisms of interaction and evolution allows the mitigation of unforeseen dependencies. This emphasizes the criticality of technology as central to organizational information infrastructures in order to maintain and support alignment between organizational structures and objectives. A lack of understanding of the coupling between technology and work practice exposes organizations to evolutionary hazards. It inhibits opportunities for redundancy and diversity strengthening organizational resilience to complex socio-technical failures.

Finally, how technology innovation exposes communities of practices to common hazards by reducing their diversity. The analysis at macroscopic level of socio-technical systems highlights contingencies between emerging social networks and technology. It identifies a class of hazards due to mechanisms that similarly expose the limitations of performativity,¹⁶ hence, *performativity Hazards*. The combination of negative feedback with imitation behavior in social networks let vulnerabilities to emerge. This combination results in reduced diversity across social networks and strengthening of vulnerabilities and gives rise to socio-technical failures. Note that similar mechanisms in the presence of positive feedback introduce resilience in socio-technical systems.

The analysis about how social aspects of responsibility and trust interact with technology systems enables us to deal with emerging socio-technical hazards.

These three classes of socio-technical hazards cross the various dimensions of technology risk. They enable a socio-technical analysis of risk. The remainder of this section discusses these socio-technical hazards.

Boundary hazards

Developing and implementing new organizational information systems necessarily involve reaching agreement, implicitly or tacitly, about knowledge. Various decisions affect how to classify information, how to represent it through the choice of boundary objects and how to access it. The detailed focus upon the design, implementation and use of information systems allows us to consider various opportunities that may exist whether in terms of improved change management procedures or systems to deploy information systems effectively and dependably. Organizations adopt different strategies in order to deal with similar problems with respect to information infrastructures, or boundary objects (infrastructures). Technology solutions address this problem differently, some times, locally or, alternatively, at an organizational level. In other cases, organizations adopt existing solutions as established standards or classification systems. However, transfer of knowledge, from its local origin to a standardized classification, or across organizational boundaries and divisions of labor, may affect local knowledge and undermine currently existing work practices. Organizations failing to understand and to treat boundary objects (infrastructures) carefully are likely to experience disruptive consequences, which represent significant threats to the dependability of information systems. These hazards may affect knowledge with potential critical consequences for organizational activities and objectives. Technology integration and standardization, or innovation strategies, although they often involve solutions (for example, Commercial Off-the-Shelf (COTS) systems) outside direct scrutiny, expose organizations to a set of hazards across organizational boundaries or divisions of labor, hence *boundary hazards*.

Boundary objects and infrastructures

Boundary objects arise at the intersection of different communities of practice, who recognize shared boundary objects. Boundary objects capture trade-offs between *generality* and *locality*. On the one hand, they capture *explicit knowledge* (Vincenti, 1990) as generally recognized by communities of practice. On the other hand, they also require *procedural knowledge* (Vincenti, 1990) in order to make boundary objects effective and available into specific localized situations. Communities of practice tailor them in order to satisfy local requirements. Therefore, boundary objects emerge over time due to *naturalization* (for example, cooperation and negotiation) by different

communities of practice (Bowker and Star, 1999). The adoption of boundary objects involves the process of naturalization of the object within communities of practice. Whereas, *membership* to a community of practice requires the recognition of boundary objects as work practices (Bowker and Star, 1999). Characterizing spatio-temporal dynamics of a classification involves reconstructing its *trajectory*. Trajectories capture the relationships, that is, membership and naturalization, between objects and communities of practice (Bowker and Star, 1999). They capture the negotiation and shaping of boundary objects of different communities of practice. The negotiation of boundary objects (for example, the negotiation of different classifications) identifies trajectories as being spatio-temporal ordered representational states (Bowker and Star, 1999; Ackerman and Halverson, 2004). The negotiation process (between communities of practice) needs to address conflicts (for example, belonging to different categories) arising among different classifications.

The *coupling* between boundary objects and communities of practice depends on the naturalization of boundary objects within the community of practice as well as of the membership of communities of practice with respect to boundary objects. These relationships create subtle mechanisms of interactions between boundary objects and communities of practice (and themselves, respectively). They are pervasive and ubiquitous among communities of practice sharing them. On the one hand, boundary objects identify communities of practice. On the other hand, communities of practice identify themselves with boundary objects. Collections of boundary objects and their relationships with communities of practice create *complex* networks of boundary objects, called, *boundary infrastructures* (Bowker and Star, 1999). Coupling and complexity of technical systems provide a framework for the characterization of risk (Perrow, 1999). The issue of whether its the technology or its the management regimes seems important. For example, complex and tightly couple management structures is probably what causes some problems with complex systems – the system, though complex, probably functions to specification. Similarly, the tight coupling between boundary objects and communities of practice and the complexity of boundary infrastructures emphasize how organizational boundaries represent a hazard or source of risk of technological systems. As structures emerge in technical systems, boundary objects of communities of practice harden the coupling and complexity of such systems. Investigating the underlying mechanisms enhances our understanding of boundary objects as enabling technologies for dependability (Lutters and Ackerman, 2002).

Classification systems and standards

Classification systems, or simply *classifications*, provide a socio-technical viewpoint in order to analyze technological systems (Bowker and Star, 1999). They technically represent (partially) ordered systems consisting of categories, which provide us with ‘a spatial, temporal or spatio-temporal segmentation of the

world' (Bowker and Star, 1999). Classifications as *information infrastructures* enable the cooperation between different *communities of practice*. It is possible to analyze classifications in terms of boundary objects as resulting from the social and political mediation between different communities of practice. Looking at classifications as arising from mediation of social and political communities allows the analysis of information infrastructures and boundary objects. The analysis emphasizes the crucial role of classifications in enabling work practice as well as communication and cooperation between different communities. It is possible, therefore, to analyze classifications as result of complex socio-technical relationships. This highlights the evolutionary nature of classifications.

Classifications, such as information systems or infrastructures, are ubiquitous and pervasive in many professional and application domains. They provide a means for categorizing and gathering information that constitutes *knowledge* in our 'modern state' (Bowker, 1996) or 'risk society' (Beck, 1992). On the one hand, classifications represent practical tools used in diverse application domains. On the other hand, classifications capture information flows in systems as well as organizations. From a system viewpoint (Hughes and Hughes, 2000), the classification of *faults*, *errors* and *failures* enables us with causal analysis in order to investigate and assess (system) failures (Johnson, 2003; Avizienis *et al*, 2004). The identification of system vulnerabilities allows us to classify and assess technical risks (Neumann, 1995). However, the understanding of faults, errors and failures depends on cultural aspects peculiar to the application domain (specifying their definitions or meanings). Classification systems, therefore, are tightly coupled with their origin domains and their culture. They are the result of technical as well as socio-political struggles addressed over the years.

Standards are related to classifications, however, differ from classifications in the way they are, imposed some times, resistant to change and adopted by different communities of practice (Bowker and Star, 1999). Communities of practice characterize (or recognize) themselves by adopting or sharing different classifications or standards. Therefore, resulting classifications depend on the mechanisms of shaping them and the policies characterizing communities. As risk is a social and collective construct (Douglas and Wildavsky, 1982), so classifications are. Classifications, as well as standards, emerge from the negotiation of diverse communities of practice. They allow information to be spread across organizational boundaries. They reside in the intersection between communities of practice, therefore, they are boundary objects (Bowker and Star, 1999).

Classifications in health care

The *international classification of diseases* (ICDs), adopted and maintained by the World Health Organization (WHO), emerged as a means for monitoring

and analyzing diseases and their developments (Bowker, 1996; Bowker and Star, 1999). It is one of the classifications forming the *WHO Family of International Classifications*, which provides practical tools for classifying diseases, monitoring their spread over populations, decision making and policy outlining (for example, identifying contingency measures for isolating diseases; World Health Organization, June 2004). The history of the ICD shows dependencies between the development of the classification and technology (Bowker, 1996). The better our understanding of their interdependencies, the better our ability to design technology systems that rely on classifications.

Another example drawn from classification practices in a healthcare domain is the study in Hardstone *et al*, 2006 and Anderson, 2008 that analyzes the introduction of an integrated *patient information management system* (PIMS) across different heterogeneous units. The system is to provide three main functionalities: (1) it records patient information; (2) system users may retrieve several historical information about their work practices; (3) finally, the system allows users to analyze data in order to support decision-making and evidence-based clinical practices. The study focused on one component, namely, the *contact purpose menu*, of the new system (Hardstone *et al*, 2006; Anderson, 2008). It allows users to select among different options from a pull-down menu of activity descriptions. Figure 1 shows some of the categories (forming a classification system) drawn from the contact purpose menu (Anderson, 2008). The field is mandatory for each clinical contact. The customization and evolution of this menu resulted to be critical for the creation of an integrated information infrastructure. The initial version of the menu simply integrated different options from different existing menus, assuming that the meaning of each option would have been shared among different users and across organizational boundaries and divisions of labor.

Studies like the one reported in Hardstone *et al*, 2006 and Anderson, 2008 allow us to highlight boundary objects and their mechanisms with respect to communities of practice and technological systems. Lack of understanding of boundary objects and failure to take subtle processes and interaction mechanisms into account in designing and deploying new technology represent potential hazards for technological systems. The analysis enhances our ability to understand boundary objects in technological systems and their related risk.

Evolutionary hazards

The evolutionary nature of technology highlights three different classes of *evolutionary hazards*: *evolving work practices*, *understanding technology trajectories* and *judging moving targets*. Various studies (Hartswood, 2002a,b; Voss, 2002a,b) highlighted the coupling between technology and work practice. In particular, work practice and technology coevolve. On the one hand,

Assessment
Case conference
Challenging behaviour
Cognitive behavioural therapy
Depot medication
Detox
Discharge
Enabling
Epilepsy
Follow-up
Full assessment
Health promotion
Initial assessment
Lawyer/solicitor report
Maintenance
Management
Mental health assessment
Methadone contract signing
Methadone programme
Methadone review
Not specified
Other report
...

Figure 1: Categories in a contact purpose menu.

technology evolution is driven to some extent by technological innovations. On the other hand, technology innovation is often characterized by social groupings engaging technological as well as political arguments. This emphasizes the criticality of technology as central to organizational information infrastructures in order to maintain and support alignment between organizational structures (for example, in terms of divisions of labors) and objectives (for example, strategic business targets). Failing to understand the coupling between technology and work practice poses risk to technology evolution. A lack of understanding of subtle relationships between technology and work practice creates mistrust in technology innovation. Moreover, mechanisms of technological evolution concern divisions of labor, which may exploit, intentionally or accidentally, technology innovation in order to alter organizational boundaries, for example, by shifting responsibilities. It is also important to understand how technology innovation (by embedding knowledge into boundary objects or infrastructures) supports formal as well as informal organizational knowledge supporting communities of practice. Failing to address evolving work practice – technology innovation – exposes organizations to (evolutionary) hazards and inhibits opportunities for redundancy and diversity

strengthening organizational resilience to complex socio-technical interaction failures.

Technology trajectories

Technology trajectories emerge as results of evolutionary negotiations involving communities of practice. These negotiations, although involving an extent of technical arguments, involve design decisions as well as social struggles. However, technology innovation consists of cycles of discoveries and exploitations. Further understanding these underlying cycles and mechanisms of technology evolution enhances our ability of managing and configuring technology innovation.

Different organizations focus technology innovation strategies toward informatization, formalization and standardization activities. They are concerned with the need to address the dynamics of standardization (encompassing both the formation and implementation of standardization), though organizations face problems of working with evolving classifications. Understanding the underlying dynamics enhances our ability to analyze evolutionary, as well as boundary, hazards, which are relevant for designing and evolving technology innovation. For instance, the introduction of standardization, which can yield a sense of increasing general accountability, highlights discrepancies between standard scheme and local practice (rooted in existing heterogeneous information structures and practices). It is possible to identify different innovation strategies. For instance, technology innovation changes how organizations interact and negotiate knowledge. A scrutiny and control over global activities may also be accompanied by a loss of local focus and detail oversight. The organizational alignment process may, initially, encounter resistance in the organizations. This may be a source of new undependabilities. The contradictory effects of standardization efforts go to the heart of questions of trust, in particular, to the (misplaced) assumption that standardized information structures and practices can resolve the problems of trust in complex and (spatially and culturally) dispersed organizational settings.

This highlights how the complexity of technology resides in subtle interactions of evolution taking into account emergent organizational (for example, social) relationships. Socio-technical relationships extend technology complexity and innovation. This requires us to understand, one the one hand, drivers of technology evolution, as well as, on the other hand, emerging (engineering) knowledge registering any socio-technical shifts. These shifts expose the limitations of assessing technology innovation. Moreover, they inhibit our ability of advocating and arguing technology innovation. Capturing these complex interactions enhances our ability of constructing, reusing and changing (safety) arguments (for example, see Smith and Harrison, 2003, 2005; Felici, 2006a). This requires us to unveil technology underlying

complexity. Understanding mechanisms of interaction and evolution intends to some extent to mitigate *unforeseen* dependencies. This makes the problem of assessing technology innovation theoretically difficult and complex (for example, reliability assessment of COTS upgrades (Popov, 2002; Popov and Littlewood, 2004)). System failures or emerging knowledge may often invalidate our assumptions (Felici, 2006a). They require the renegotiation of structured technology arguments (for example, multilegged arguments (Bloomfield and Littlewood, 2003, 2006). Moreover, underlying evolutionary processes require us to adapt engineering knowledge and the construction of supporting (dependability) arguments for technology innovation.

Performativity hazards

The study of socio-technical systems at macro level highlights contingencies between emerging social networks and overall system properties. The results drawn from the study of the limitations of the performativity of economics stress the social aspects of large-scale systems. The social nature of finance (stressed by the distinction between *N-terms* and *S-terms*)¹⁷ highlights similarities between modern financial markets and large socio-technical systems (MacKenzie, 2001b). The emergence of social connectivities (for example, mutual susceptibility, imitation and hard networks), or generally speaking social networks, characterizes global financial markets (MacKenzie, 2004b). Mechanisms (for example, performativity and counterperformativity) underlying and emerging in social networks expose the limitations of technological accounts of socio-technical systems (MacKenzie, 2003a, 2004a). Similar limitations arise for the performativity of financial markets due to the emerging behavior spreading across social networks (MacKenzie, 2003b; MacKenzie and Millo, 2003). On the other hand, emerging social networks expose the limitations of purely technological (or theoretical) accounts of such systems. In particular, socio-technical systems – at macro level – exhibit particular properties due to emerging social networks. Social networks extend technology. The analysis of such properties allows us to identify as class of hazards due to mechanisms that similarly expose the limitations of performativity,¹⁸ hence, *performativity hazards* (for example, *positive* or *negative feedback* and *imitation behavior*). Socialities expose the limitations of system performativity (for example, that system is what is declared to be) by the emergence of positive (negative) feedback. On the one hand, positive feedback may strength system features (for example, stability, dependability and so on). On the other hand, negative feedback may undermine system features and expose organizations to failures. It is also important to understand how social connectivities extend technical systems and how technology mediates social interaction. Therefore, understanding the nature of the social connectivities involved and supported by technology is necessary. Furthermore, social

connectivity affects the perception of risk with respect to technology. Organizational structures (for example, social networks) make system susceptible and vulnerable to collective actions resulting in imitating behavior. The emergence of imitating behavior affects system diversity and reduces independence across communities of practice.

The combination of negative feedback with imitation behavior in social networks, that is, emerging social connectivities, let undependabilities to emerge. This combination results in reduce diversity across social networks and strengthening of vulnerabilities and gives rise to (socio-technical) failures. Note that similar mechanisms in presence of positive feedback introduce resilience in socio-technical systems. Moreover, the hardening of social relationships creates stable social networks. This process is similar to the one of creating stable communities of practice around boundary objects. Therefore, communities of practice build strength by adopting technology, although they became vulnerable in presence of negative feedback that undermines system dependability.

Social connectivity

How do features emerge in socio-technical systems? What are means of propagation in socio-technical systems? The theory of classification (Bowker and Star, 1999) explains how communities of practices identify themselves with adopted technological artifacts or boundary objects, hence boundary infrastructures. The social shaping of technology theory (MacKenzie and Wajcman, 1999) explains how people shape technological artifacts and drive technology evolution, hence technology innovation. *What is then the missing link? How does the IS build up?* It is, therefore, necessary to unveil the mechanisms that make us behaving not just like individuals, but behaving like social ‘animals’ (Strum and Latour, 1987; MacKenzie and Wajcman, 1999). It is necessary to move the analysis from the *micro*, that is, understanding how individuals, or social actors, behave with respect to technology, to the *macro*, that is, understanding how societies, or social groups, behave with respect to technology.

Looking at the micro scale of socio-technical systems, *distributed cognition* (Norman, 1993; Halverson, 2002) takes into account how social actors acquire and use resources. Distributed cognition (Norman, 1993; Halverson, 2002) focuses on the interaction between representational resources, which can be located within human mind as well as external artifacts. It enhances our understanding of how people carry on information-mediated activities by using distributed resources. Distributed cognition stresses that human cognition is not isolated within human minds, but it emergently extends to external distributed artifacts. Internal and external artifacts do not exist in isolation – they are integral parts of socio-technical systems. A holistic view of socio-technical systems captures the nature of socio-technical systems. The

characterization of distributed cognition provides us a simple systemic model of socio-technical systems. *Activity theory* (Halverson, 2002; Kaptelinin and Nardi, 2006), on the other hand, analyzes how *social interactions* influence human cognition. Activity theory explains how human beings regulate their behavior by means of inclusion of auxiliary stimuli into their activities. The stimuli take origin in external artifacts or in social interactions. In other words, activity theory emphasizes that human behavior should be understood in the context of social interactions and external activities. Any subject (or individual) accomplishes specific activities (or objectives) through negotiations within a social community by processes of *internalization* and *externalization*. Internalization explains how individuals construct internal models of their activities (to be performed). Externalization explains how individuals design and implement new activities. Communities of practices adopt similar processes (that is, membership and naturalization) in shaping boundary objects, that is, artifacts shared by communities. Similarly, processes of *social learning* explains how human beings perceive machines in order to acquire computational artifacts and to accomplish specific activities (or tasks; Williams *et al*, 2005). Social learning, in particular, consists of two main processes, namely, *innofusion* (that is, learning by trying) and *domestication* (that is, learning by interacting). The combination of distributed cognition and activity theory enables us to characterize socio-technical systems, although it is yet necessary to enhance our ability to 'go beyond description to prediction' (Halverson, 2002) of emergent socio-technical systems. It is, hence, important to understand how social networks (Klein and Kleinman, 2002; Nardi *et al*, 2002; Churchill and Halverson, 2005; Licoppe and Smoreda, 2005;) shape technology and let system properties (for example, dependability) to emerge.

Social actors, therefore, use available resources in order to achieve specific objectives and perform their activities within emerging social structures or networks (Nardi *et al*, 2002; Churchill and Halverson, 2005). Technology mediated social networks characterize modern societies (hence, for example, *information society*). Research in social networks investigate networking properties in order to support the design of technology (Churchill and Halverson, 2005). Sociological accounts, for instance, giving rice to ANT (Strum and Latour, 1987; MacKenzie and Wajcman, 1999; Latour, 2003), explain the social link between *social actors* and heterogeneous entities (for example, classification systems Bowker and Star, 1998). Social actors perform within their social networks. These *spontaneously emerging* social networks (for example, intentional networks Nardi *et al*, 2002) are essential in the modern technology mediated society. They exploit available *resources* in order to organize other social actors on a large scale (Strum and Latour, 1987). Moreover, social processes used for engaging within emerging structures affect risk perception (Douglas and Wildavsky, 1982). Therefore, a lack of account of such social networks and group formation exposes socio-technical systems to

a set of emerging socio-technical hazards – complementary to purely technical hazards – due to the nature of such systems. For instance, at the micro level, interactions may give rise to socio-technical hazards related to timing and knowledge distribution (Filipe *et al*, 2003), that is, micro level interactions. On the other hand, at the macro level, people (with their social networks) may constrain socio-technical systems by collective behavior and give rise to emergent properties. The analysis of socio-technical systems in the large, that is, at the macro level, enhances our understanding of mechanisms underpinning social networks and affecting socio-technical systems.

Discussion and Conclusions

Social aspects of technology enhance our understanding of *emerging technological risk*. In particular, a social perspective to technology enables the underpinning of various classes of technology hazards, namely, *boundary hazards*, *evolutionary hazards* and *performativity hazards*, complementing current risk assessment methodologies. Figure 2 shows a representation of the manifestations of the three classes of socio-technical hazards as tensions (or propagation directions) between organization and technology. *Boundary hazards* (1) highlight the vulnerabilities of organizational boundaries. Technology often exposes organizations to the propagation of hazards across organizational boundaries. Moreover, the risk lays also in the shift of responsibilities across organizational boundaries and in the rising of mistrust across divisions of labor. *Evolutionary hazards* (2) emerge in a lack of understanding technology trajectories as results of social shaping of technology. Finally, technology nowadays mediates social connectivities. On the other hand, social networks extend technology and expose organizations to emerging hazards (for example, negative feedback and imitation behavior), which could contribute toward hardening social links and establishing hard homogeneous communities reducing diversity and structural resilience, hence *performativity hazards* (3).

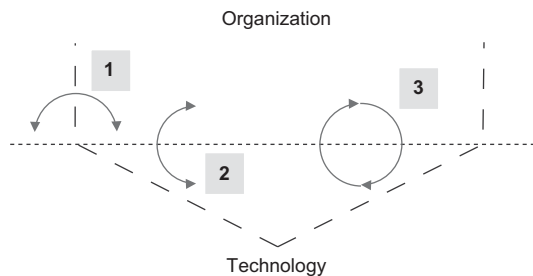


Figure 2: Tensions of socio-technical hazards.

These classes of socio-technical hazards allow the characterization of emerging technological risk in complex organizational settings. The classes of identified socio-technical hazards (that is, boundary, evolutionary and performativity hazards) provide, that is, underpin, a characterization about the risk of technology innovation. The findings extend, that is, complement technology-driven risk analysis.

Emerging technological risk – expressed in terms of *boundary hazards*, *evolutionary hazards* and *performativity hazards* – enhances our understanding of technology innovation. It allows us to analyze the risk involved with technology innovation. This complements and extends technology risk analysis. A lack of understanding of the basic mechanisms inhibits and undermines technology innovation. Moreover, it exposes organizations to technology risk. This manifests, for instance, as weak organizational knowledge or problematic technology interaction. The underpinning of emerging technological risk enhances our understanding about how basic socio-technical mechanisms expose organizations to technology hazards. This provides new insights and understandings of emerging technological risk. The better our understanding of emerging technological risk, the better our ability to deploy technology enabling communities of practices, hence, *hardening social links*. However, it is necessary to understand how technology innovation exposes organizations to new classes of socio-technical hazards. On the other hand, social aspects of technology expose the limitations of pure technological dependability arguments. Studies of the underlying mechanisms draw some general lessons for understanding and addressing emerging technological risk. In conclusion, this paper reviews diverse accounts of technology risk. Moreover, it identifies *new* classes of socio-technical hazards, namely, *boundary*, *evolutionary* and *performativity hazards*. These hazards derive from socio-technical accounts of technology risk. The combination of these hazards together with the diverse risk accounts identifies a framework, which enhances microscopic and macroscopic levels of risk analysis.

Acknowledgements

This work has been supported by the UK EPSRC Interdisciplinary Research Collaboration in Dependability (DIRC) – <http://www.dirc.org.uk> – Grant GR/N13999, and by the Interdisciplinary Design and Evaluation of Dependability (INDEED) – <http://www.indeedproject.ac.uk> – Grant EP/E001297/1.

Notes

- 1 The problem is then to establish or interpret a link between different levels of analysis: (Le Coze, 2008) 'It must be acknowledged however that no conflicting view is implied here between human factors (a micro level) and organisational factors (a meso-macro level) as it is believed that by principle links do exist between the two approaches. The difficulty is however a well known interdisciplinary and scientific difficulty where individual levels with for example psychological

- land psycho-cognitive insights and a higher level with sociological, psycho-sociological or anthropological dimensions need conceptual and empirical articulations.’
- 2 Diverse approaches and methodologies pinpoint different risk accounts as well as identify different practices of investigating technology risk (Le Coze, 2008): ‘These two positions descriptive and normative help defining a continuum along which different investigation processes (implying different type of rationales, resources, models, time and access of information but also purposes and method) can be unfolded, depending on the context of the accident, its scope but also on the resources and competence of the people in charge of applying the tools and methodologies.’
 - 3 Complex causalities characterize the social dimensions of technology: (Le Coze, 2008) ‘Complexity [...] provides a pictures of the human and social world where causalities are not linear, where their effects can be by nature unpredictable and counter intuitive. The nature of this unpredictability is found in the high number of interrelated, self-organized entities that are always affected by changes in the system, through interactions and feedbacks, and thus leading to unexpected and emergent pat-terns. Circular causalities [...] are a more suitable approach than a linear one when it comes to thinking of causalities in the social and human world, and therefore in organisations. These evolutions are not fully predictable, and future is consequently hardly deterministic when it comes to organisations.’
 - 4 Rogers *et al* (2005) questions the nature of *interdisciplinarity* as well as *multidisciplinarity*. Although multidisciplinary work often faces difficulties in practice, it stresses how multidisciplinary work could be a strategy for overcoming limitations ‘within’ single disciplines. The adaptation of artifacts (for example, models, concepts and so on) drawn from other disciplines into an integrated framework support the seeking of understanding complex problems, which remain unresolved or incomprehensible within single disciplines. These mechanisms allow us to tackle complex, otherwise unresolved or incomprehensible, problems into emerging *interdisciplinary* accounts, which characterize *solutions* into an integrated framework arising from diverse disciplines and filling knowledge gaps within and between disciplines.
 - 5 ‘A *hazard* is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event)’, p. 177, (Leveson, 1995). ‘*Risk is the hazard level* combined with (1) the likelihood of the hazard leading to an accident (sometimes called *danger*) and (2) hazard exposure or duration (sometime called *latency*)’, p. 179, (Leveson, 1995).
 - 6 Avi-zienis *et al* (2004) introduces the basic concepts of *dependability* and *security*. It, in particular, revises the definition of system dependability – ‘the ability to deliver service that can justifiably be trusted’ – in an alternative one: ‘the ability to avoid service failures that are more frequent and more severe that is acceptable’. Basic attributes (that is, *availability, reliability, safety, confidentiality, integrity* and *maintainability*) refine the notion of dependability. Note that security is defined in terms of availability, confidentiality and integrity. This relates security to dependability into an integrated framework. The basic definitions allow the discussion of the main threats (that is, *faults, errors* and *failures*) to dependability and security. It, then, introduces the main means (that is, *fault prevention, fault tolerance, fault removal* and *fault forecasting*) to achieve dependability and security. All definitions and concepts form a framework for dependability and security: *the dependability and security tree*.
 - 7 ‘Linear interactions are those in expected and familiar production or maintenance sequence, and those that are quite visible even if unplanned’ – ‘Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible’ (Perrow, 1999, p. 78).
 - 8 ‘Descriptive knowledge, as the term suggests, describes things as they are. Prescriptive knowledge, by contrast, prescribes how things should be to attain a desired end.’ They ‘denote varieties of explicit knowledge. To these, we must add [...] tacit knowledge [...]. Tacit knowledge and prescriptive knowledge [...] can thus both be describe as procedural knowledge [...]’ (Vincenti, 1990, pp. 197–198).
 - 9 The *Social Shaping of Technology* (SST; Williams and Edge, 1996; MacKenzie and Wajcman, 1999) identifies the mechanisms underlying the social design and implementation of technology. It questions any distinction between technical and social accounts of technology.

- 10 The 'man-made disasters model' stresses that information difficulties as barriers inhibit organizational learning (Pidgeon and O'Leary, 2000). It identifies four types of information difficulties (Pidgeon and O'Leary, 2000): (1) latent or misunderstood critical errors or events, (2) dangerous preconditions in ill-structured and constantly changing situations, (3) uncertainty and (4) minimization of danger despite emerging information or signals working.
- 11 The investigations of industrial case studies drawn from the industrial manufacturing domain highlight how software artifacts allow the integration of organizational knowledge (D'Adderio, 2001). *The transfer of knowledge* into software artifacts involves processes of generalizations and contextualizations. These processes, moreover, enable the coordination and communications between different organizational units, or communities of practices (for example, engineers and designers). Therefore, embedding organizational knowledge into software artifacts involves a coevolutionary process. On the one hand, knowledge acquisition and generalization involve processes of codification and simplification. On the other hand, knowledge utilization involves processes or reinstatement of subjectivity and local knowledge.
- 12 The theory of *remodernization* advocates the existence of diverse modernities (Latour, 2003). The analysis of remodernization draws a comparison between the *actor-network theory* (ANT) and the *risk society*. The work by Latour (2003) rejects the term *modern* as often advocated by technologists. It argues that, on the contrary, we 'have never been modern'. It analyzes features (for example, reflexive behaviors, externalities and so on) of 'modern' societies with respect to the similarities and differences between ANT and risk theory. It argues that although remodernization might be or not be happening, evidence is still patchy. Finally, it points out similarities and differences between the ANT and the risk society.
- 13 A possible (hierarchical) classification of the performativity of economics consists of (MacKenzie, 2006): 'generic' performativity, 'effective' performativity, 'Barnesian' performativity and counterperformativity 'generic' performativity: an aspect of economics (a theory, model, concept, procedure, data set and so on) is used by participants in economic processes, regulators and so on; 'effective' performativity: the practical use of an aspect of economics has an effect on economic processes; 'Barnesian' performativity: practical use of an aspect of economics makes economic processes more like their depiction by economics; counter performativity: practical use of an aspect of economics makes economic processes less like their depiction by economics.
- 14 For instance, a 'safety culture' arises in a High Grid High Group setting, because there is high internal cohesion and stringent demands on accountability to external authorities, so a particular regime involving audit and transparency evolves. This situation is present to a certain extent in the organizational structures and relationships between Air Traffic Management providers and Civil Aviation Authorities. Comparing the 'safety culture' in health care (in terms of organizational structures and relationships), which is much less transparent and is only made accountable in extreme cases through the law.
- 15 This correlation manifests in the presence of subcultures (Health & Safety Laboratory, 2002): 'Subcultures are likely to develop when employees within the same organisation experience different working conditions. Work groups within an organisation are likely to view risk differently depending on the type of work they do. In general, subcultures are not seen as undesirable and it can be argued that they provide useful contextual insight into the different risk and hazards experienced by workgroups.'
- 16 Performativity is a term coined by MacKenzie (MacKenzie, 2006) to describe the situation where behaving 'as if' the world is a particular way brings about changes that draw the world closer to the 'as if' world. One example here, is the development of the 'just in time' approach to logistic chains. This has led the world to be dominated by de-stocked, lightweight, high-speed logistic chains. In the climate of the late twentieth century, the 'real world' was aligned with the assumptions underlying this model. Now, a few years on supply chains look vulnerable, and de-stocking may not be the best approach for some kinds of commodity. Similarly, in finance, the development almost universal practice of unsecured inter-bank lending led to a glut of credit in the early twenty-first century that led to a correction in 2007–2008.
- 17 It is possible to characterize the distinction between the social and the technical, similarly to the distinction between *N-type* (natural kind) and *S-type* (social kind) terms. In the analysis of arbitrage in the case of *long-term capital management*, MacKenzie stresses the performative nature

of finance by showing the presence of S-type terms: *An N-type, or natural kind, term is one in which the application of the term to a particular entity can be thought of as a process in which the empirical properties of the entity are judged against a pattern, and the term is applied or not applied according to the perceived closeness of fit. [...] In contrast, with an S-type, or social kind, the process of concept application is performative [...]* (MacKenzie, 2001, p. 126).

- 18 Performativity tends to draw the behavior of the world towards the expected model-but this is always provisional-for example there is usually an assumption that all things have a price because there is always liquidity and so someone is able to get money to buy things (even if the are very cheap or very expensive). This stopped happening during the subprime crisis and Banks started to say they couldn't price assets because there was no market (there are many ways to price an asset that doesn't have to do with a market – but Bankers aren't used to anything other than a market). Hence, the central Banks try to pump money into the system to get things moving but a number of assumptions have changed and so its harder to get the whole thing going again.

References

- Ackerman, M.S. and Halverson, C.A. (2000) Reexamining organizational memory. *Communications of the ACM* 43(1): 59–64.
- Ackerman, M.S. and Halverson, C.A. (2004) Organizational memory as objects, processes, and trajectories: An examination of organizational memory in use. *Computer Supported Cooperative Work* 13(2): 155–189.
- Adam, B., Beck, U. and Loon, J.V. (eds.) (2000) *The Risk Society and Beyond: Critical Issues for Social Theory*. London, Thousand Oaks, New Delhi: SAGE Publications.
- Anderson, R. and Moore, T. (2006) The Economics of information security. *Science* 314: 610–613.
- Anderson, S., Hardstone, G., Procter, R. and Williams, R. (2008) Down in the (data)base (ment): Supporting configuration in organizational information systems. In: M.S. Ackerman, C.A. Halverson, T. Erickson and W.A. Kellogg (eds.) *Resources, Co-Evolution and Artifacts: Theory in CSCW*. London: Springer-Verlag, Chapter 9, pp. 221–253.
- Arlat, J. et al. (1998) *Dependability Handbook*, Technical Report 98–346, LAAS-CNRS, LIS, Toulouse.
- Atkinson, C., Eldabi, T., Paul, R.J. and Pouloudi, A. (2001) *Investigating Integrated Sociotechnical Approaches to Health Informatics*, Proceedings of the 34th Hawaii International Conference on System Sciences, HI: IEEE Press, pp. 1–10.
- Aven, T. and Kristensen, V. (2005) Perspectives on risk: Review and discussion of the basis for establishing a unified and holistic approach. *Reliability Engineering & System Safety* 90(1): 1–14.
- Avizienis, A., Laprie, J.-C., Randell, B. and Landwehr, C. (2004) Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 1(1): 11–33.
- Beck, U. (1992) *Risk Society: Towards a New Modernity*. London, Thousand Oaks, New Delhi: SAGE Publications.
- Beck, U., Bonss, W. and Lau, C. (2003) The theory of reflexive modernization: Problematic, hypotheses and research programme. *Theory, Culture & Society* 20(2): 1–33.
- Bloomfield, R. and Littlewood, B. (2003) *Multi-Legged Arguments: The Impact of Diversity upon Confidence in Dependability Arguments*, In: Proceedings of the 2003 International Conference on Dependable Systems and Networks, DSN'03, IEEE Computer Society: IEEE Press, pp. 25–34.
- Bloomfield, R. and Littlewood, B. (2006) On the use of diverse arguments to increase confidence in dependability claims. In: D. Besnard, C. Gacek C.B. Jones (eds.) *Structure for*

- Dependability: Computer-Based Systems from an Interdisciplinary Perspective*. London: Springer-Verlag, Chapter 13, pp. 254–268.
- Borodzicz, E.P. (2005) *Risk, Crisis & Security Management*. Chichester, UK: John Wiley & Sons.
- Bottitta, S. and Felici, M. (2006) Understanding and learning trust: A review, characterization and tool. In: C.G. Soares and E. Zio (eds.) *Safety and Reliability for Managing Risk*, Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006), vol. 2, Estoril, Portugal: Taylor & Francis Group, pp. 1273–1280.
- Bowker, G.C. (1996) The history of information infrastructures: The case of the international classification of diseases. *Information Processing & Management* 32(1): 49–61.
- Bowker, G.C. and Star, S.L. (1998) Building information infrastructures for social worlds – the role of classifications and standards. In: T. Ishida (ed.) *Community Computing and Support Systems*, No. 1519 in LNCS, Berlin: Springer-Verlag, pp. 231–248.
- Bowker, G.C. and Star, S.L. (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA; London: The MIT Press.
- Churchill, E.F. and Halverson, C.A. (2005) Social networks and social networking: Guest editors' introduction. *IEEE Internet Computing* 9(5): 14–19.
- D'Adderio, L. (2001) Crafting the virtual prototype: How firms integrate knowledge and capabilities across organisational boundaries. *Research Policy* 30(9): 1409–1424.
- D'Adderio, L. (2003a) Configuring software, reconfiguring memories: The influence of integrated systems on the reproduction of knowledge and routines. *Industrial and Corporate Change* 12(2): 321–350.
- D'Adderio, L. (2003b) *Inside the Virtual Product: How Organisations Create Knowledge Through Software*. Cheltenham, UK Northampton, MA: Edward Elgar.
- Douglas, M. and Wildavsky, A. (1982) *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. Berkeley and Los Angeles, CA; London: University of California Press.
- Felici, M. (2006a) Capturing emerging complex interactions: Safety analysis in air traffic management. *Reliability Engineering & System Safety* 91(12): 1482–1493.
- Felici, M. (2006b) Trust strategies: Motivations from the air traffic management domain. In: C.G. Soares and E. Zio (eds.) *Safety and Reliability for Managing Risk*, Proceedings of the European Safety and Reliability Conference 2006 (ESREL 2006), vol. 3, Portugal: Taylor & Francis Group, pp. 1797–1804.
- Felici, M. (2007) Trust strategies and policies in complex socio-technical safety-critical domains: An analysis of the air traffic management domain. In: N. Guelfi, D. Buchs (Eds.) Proceedings of the 3rd International Workshop on Rapid Integration of Software Engineering techniques, RISE 2006, No. 4401 in LNCS, Geneva, Switzerland: Springer-Verlag, pp. 51–65.
- Filipe, J.K., Felici, M. and Anderson, S. (2003) Timed knowledge based modelling and analysis: On the dependability of socio-technical systems. In: Proceedings of HAAMAHA 2003 8th International Conference on Human Aspects of Advanced Manufacturing: Agility & Hybrid Automation, Roma: Consiglio Nazionale delle Ricerche, Istituto di Scienze e Tecnologie della Cognizione, pp. 321–328.
- Gigerenzer, G., Todd, P.M. and Group, T.A.R. (1999) *Simple Heuristics That Make Us Smart*. New York: Oxford University Press.
- Halverson, C.A. (2002) Activity theory and distributed cognition: Or what does cscw need to do with theories? *Computer Supported Cooperative Work (CSCW)* 11(1-2): 243–267.

- Hardstone, G., D'Adderio, L. and Williams, R. (2006) Standardization, trust and dependability. In: K. Clarke, G. Hardstone, M. Rouncefield I. Sommerville (eds.) *Trust in Technology: A Socio-Technical Perspective*, Vol. 36 of CSCW, London: Springer-Verlag, Chapter. 4 pp. 69–104.
- Hartwood, M. *et al.* (2002a) Co-realization: Toward a principled synthesis of ethnomethodology and participatory design. *Scandinavian Journal of Information Systems*. 14(2): 9–30.
- Hartwood, M. *et al.* (2002b) The benefits of a long engagement: From contextual design to the co-realisation of work affording artefacts. In: Proceedings of NordiCHI, ACM, The IRIS Association, Viktoria Institute, Box 620, SE-405 30 Göteborg, Sweden, Jens Kaaber Pors, Dixi Henriksen, Brit Ross Winthereik, Marc Berg (eds), pp. 283–286.
- Health & Safety Executive (HSE). (2001a) Social amplification of risk: The media and the public. Research Report 329.
- Health & Safety Executive (HSE). (2001b) The impact of social amplification of risk on risk communication. Research Report 332.
- Health & Safety Executive (HSE). (2002) Taking account of societal concerns about risk – Framing the problem. Research Report 035.
- Health & Safety Executive (HSE). (2005) A Review of Safety Culture and Safety Climate Literature for the Development of the Safety Culture Inspection Toolkit. Research Report 367.
- Health & Safety Laboratory (HSL). (2002) *Safety Culture: A Review of the Literature*, HSL/2002/25 Sheffield, UK: HSL.
- History of the development of the ICD, World Health Organization (WHO) Geneva, Switzerland.
- Hollnagel, E. (1993) *Human Reliability Analysis: Context and Control*. London: Academic Press.
- Hughes, A.C. and Hughes, T.P. (eds.) (2000) *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After*. Cambridge, MA; London: The MIT Press.
- Johnson, C. (2003) *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. Glasgow, UK: University of Glasgow Press.
- Kaptelinin, V. and Nardi, B.A. (2006) *Acting with Technology: Activity Theory and Interaction Design*. Cambridge, MA; London: MIT Press.
- Klein, H.K. and Kleinman, D.L. (2002) The social construction of technology: Structural considerations, science, technology. *Human Values* 27(1): 28–52.
- Latour, B. (2003) Is re-modernization occurring – and if so, how to prove it? A commentary on Ulrich Beck. *Theory, Culture & Society* 20(2): 35–48.
- Löfstedt, R.E. and Frewer, L. (eds.) (1998) *The Earthscan Reader in Risk and Modern Society*. London, Earthscan Publications.
- Le Coze, J.C. (2005) Are organisations too complex to be integrated in the technical risk assessment and current safety auditing? *Safety Science* 43(8): 613–638.
- Le Coze, J.C. (2008) Disasters and organisations: From lessons learnt to theorising. *Safety Science* 46(1): 132–149.
- Leveson, N.G. (1995) *SAFWARE: System Safety and Computers*. Boston, MA; Addison-Wesley.
- Licoppe, C. and Smoreda, Z. (2005) Are social networks technologically embedded? How networks are changing today with changes in communication technology. *Social Networks* 27(4): 317–335.
- Lutters, W.G. and Ackerman, M.S. (2002) Achieving safety: A field study of boundary objects in aircraft technical support. In: Proceedings of the 2002 ACM Conference

- on Computer Supported Cooperative Work, CSCW '2002, New York: ACM Press, pp. 266–275.
- MacKenzie, D.A. (1990) *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. Cambridge, MA; London: The MIT Press.
- MacKenzie, D.A. (1996) *Knowing Machines: Essays on Technical Change*. Cambridge, MA; London: The MIT Press.
- MacKenzie, D. (2001a) *Mechanizing Proof: Computing, Risk, and Trust*. Cambridge, MA: The MIT Press.
- MacKenzie, D. (2001b) Physics and finance: S-terms and modern finance as a topic for science studies. *Science, Technology & Human Values* 26(2): 115–144.
- MacKenzie, D. (2003a) An equation and its worlds: Bricolage, exemplars, disunity and performativity in financial economics. *Social Studies of Science* 33(6): 831–868.
- MacKenzie, D. (2003b) Long-term capital management and the sociology of arbitrage. *Economy and Society* 32(3): 349–380.
- MacKenzie, D. (2004a) The big, bad wolf and the rational market: portfolio insurance, the 1987 crash and the performativity of economics. *Economy and Society* 33(3): 303–334.
- MacKenzie, D. (2004b) Social connectivities in global financial markets. *Environment and Planning D: Society and Space* 22: 83–101.
- MacKenzie, D. (2006) *An Engine, Not a Camera: How Financial Models Shape Markets, Inside Technology*. Cambridge, MA; London: The MIT Press.
- MacKenzie, D. and Millo, Y. (2003) Constructing a market, performing theory: The historical sociology of a financial derivatives exchange. *American Journal of Sociology* 109(1): 107–145.
- MacKenzie, D. and Wajcman, J. (eds.) (1999) *The Social Shaping of Technology*, 2nd edn, Buckingham, UK: Open University Press.
- Mythen, G. (2004) *Ulrich Beck: A Critical Introduction to the Risk Society*. Sterling, VA: Pluto Press.
- Nardi, B.A., Whittaker, S. and Schwarz, H. (2002) NetWORKers and their activity in intensional networks. *Computer Supported Cooperative Work (CSCW)* 11(1–2): 205–242.
- Neumann, P.G. (1995) *Computer Related Risks*. New York: The ACM Press.
- Norman, D.A. (1993) *Things That Make Us Smart: Defining Human Attributes in the Age of the Machine*. Cambridge, MA: Perseus Books.
- Perrow, C. (1999) *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.
- Petroski, H. (1982) *To Engineer is Human: The Role of Failure in Successful Design*. New York: Vintage Books.
- Petroski, H. (1994) *Design Paradigms: Case Histories of Error and Judgment in Engineering*. Cambridge, UK: Cambridge University Press.
- Pidgeon, N. and O'Leary, M. (2000) Man-made disasters: Why technology and organizations (sometimes) fail. *Safety Science* 34(1–3): 15–30.
- Popov, P. (2002) Reliability assessment of legacy safety-critical systems upgraded with off-the-shelf components. In: S. Anderson, S. Bologna M. Felici (eds.) Proceedings of the 21st International Conference on Computer Safety, Reliability and Security, SAFECOMP 2002, No. 2434 in LNCS, Berlin: Springer-Verlag, pp. 139–150.
- Popov, P. and Littlewood, B. (2004) The effect of testing on reliability of fault-tolerant software. Proceedings of the 2004 International Conference on Dependable Systems and Networks, DSN'04, IEEE Computer Society, IEEE, pp. 265–274.

- Reason, J. (1997) *Managing the Risks of Organizational Accidents*. Aldershot, UK: Ashgate.
- Rogers, Y., Scaife, M. and Rizzo, A. (2005) Interdisciplinarity: An emergent or engineered process? In: S. J. Derry, C.D. Schunn M.A. Gernsbacher (eds.) *Interdisciplinary Collaboration: An Emerging Cognitive Science*. Mahwah, NJ: Lawrence Erlbaum Associates, Chapter. 10, pp. 265–286.
- Slovic, P. (2000) *The Perception of Risk*. London: Earthscan Publications.
- Smith, S.P. and Harrison, M.D. (2003) Reuse in hazard analysis: Identification and support. In: S. Anderson, M. Felici and B. Littlewood (eds.) Proceedings of the 22nd International Conference on Computer Safety, Reliability and Security, SAFECOMP 2003, no. 2788 in LNCS, Berlin: Springer-Verlag, pp. 382–395.
- Smith, S.P. and Harrison, M.D. (2005) Measuring reuse in hazard analysis. *Reliability Engineering & System Safety* 89(1): 93–104.
- Stoneburner, G., Goguen, A. and Feringa, A. (2002) Risk management guide for information technology systems – recommendations of the national institute of standards and technology. Gaithersburg, MD: NIST Special Publication (July) 800–30.
- Storey, N. (1996) *Safety-Critical Computer Systems*. Harlow, UK: AddisonWesley.
- Strum, S. and Latour, B. (1987) The meanings of social: From baboons to humans. *Information sur les Sciences Sociales* 26: 783–802.
- Vincenti, W.G. (1990) *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History*. Baltimore MD and London: The Johns Hopkins University Press.
- Voss, A. et al. (2002a) Dependability as ordinary action. In: S. Anderson, S. Bologna, M. Felici (eds.) Proceedings of the 21st International Conference on Computer Safety, Reliability and Security, SAFECOMP 2002, no. 2434 in LNCS, Berlin: Springer-Verlag, pp. 32–43.
- Voss, A. et al. (2002b) Accomplishing ‘just-in-time’ production. In: C. Johnson (ed.) *Human Decision Making and Control*, GIST Technical Report G2002-1, pp. 209–211.
- Williams, R. and Edge, D. (1996) The social shaping of technology. *Research Policy* 25(6): 865–899.
- Williams, R., Stewart, J. and Slack, R. (2005) *Social Learning in Technological Innovation: Experimenting with Information and Communication Technologies*. Cheltenham: Edward Elgar.
- World Health Organization (WHO). (2004) World Health Organization-Family of International Classifications.